FortifyTech
Security Assessment Findings Report

Business Confidential

Date: May 5th, 2024
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of FortifyTech and CyberShield. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both FortifyTech and CyberShield.

TCMS may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. CyberShield prioritized the assessment to identify the weakest security controls an attacker would exploit. CyberShield recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

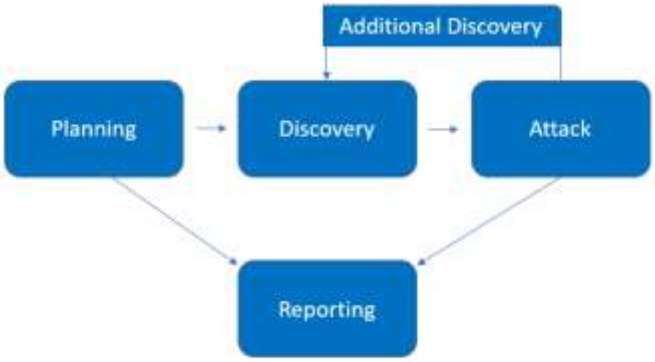
Name	Title	Contact Information
FortifyTech		
Kiseki	Information Security Consultant	Office: (555) 555-5555 Email: kiseki@fortifytech.com
CyberShield		
Jac	Lead Penetration Tester	Office: (555) 555-5555 Email: jac@cybershield.com

Assessment Overview

From May 5th, 2024 to May 8th, 2024, FortifyTech engaged CyberShield to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A CyberShield engineer performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
External Penetration Test	10.15.42.36 10.15.42.7

Scope Exclusions

FortifyTech did not give any limitations.

Client Allowances

FortifyTech did not provide any allowances to assist the testing.

Executive Summary

CyberShield evaluated FortifyTech's external security posture through an external network penetration test from May 5th, 2024 to May 8th, 2024. By leveraging a series of attacks, TCMS found medium level vulnerabilities that allowed CyberShield to discover password of admin. It is highly recommended that DC address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

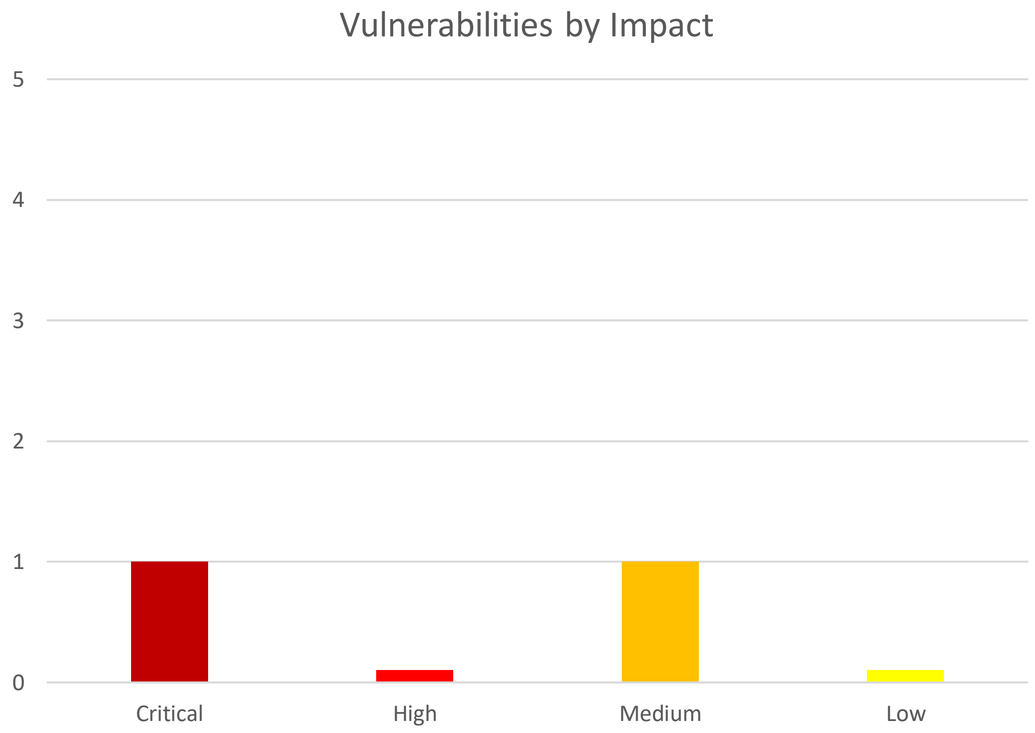
Attack Summary

The following table describes how CyberShield gained admin credentials, step by step:

Step	Action	Recommendation
1	Obtained credentials of admin through anonymous access enabled over FTP service.	Disable FTP service of anonymous.
2	Attempted a "credential stuffing" attack against Outlook Web Access (OWA), which was unsuccessful. However, OWA provided username enumeration, which allowed TCMS to gather a list of valid usernames to leverage in further attacks.	Synchronize valid and invalid account messages.
3	Performed a "password spraying" attack against OWA using the usernames discovered in step 2. TCMS used the password of Summer2018! (season + year + special character) against all valid accounts and gained access into the OWA application.	OWA permitted authenticated with valid credentials. TCMS recommends DC implement Multi-Factor Authentication (MFA) on all external services. OWA permitted unlimited login attempts. TCMS recommends DC restrict logon attempts against their service. TCMS recommends an improved password policy of: 1) 14 characters or longer 2) Use different passwords for each account accessed. 3) Do not use words and proper names in passwords, regardless of language Additionally, TCMS recommends that DC: ▪ Train employees on how to create a proper password
4	Leveraged valid credentials to log into VPN	OWA permitted authenticated with valid credentials. TCMS recommends DC implement Multi-Factor Authentication (MFA) on all external services.

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



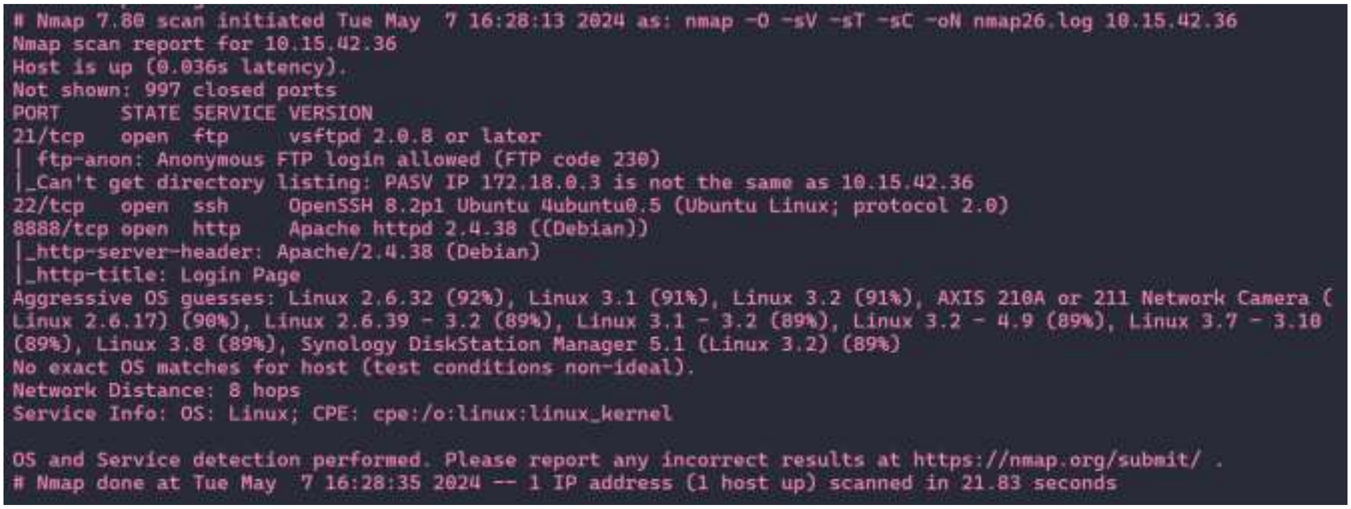
External Penetration Test Findings

Enabled Access Over FTP Service – Login (Medium)

Description:	FortifyTech enabled anonymous access over FTP service. This configuration allowed CyberShield to gain credentials of admin through its database.
Impact:	Medium (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N | Score: 5.3)
System:	10.15.42.36
References:	https://medium.com/nerd-for-tech/tryhackme-anonymous-989fb5c0edde - Enabled FTP access

Exploitation Proof of Concept

CyberShield gathered information through network scan. The network scan output shows enabled access of anonymous over FTP service (**Note:** A full list of the network scan can be found in "**Additionals**" Folder.).

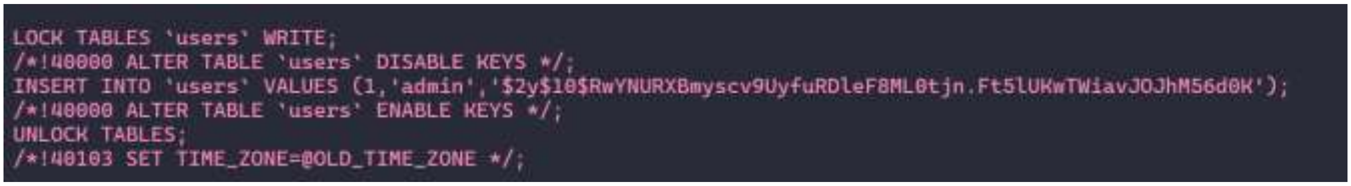


```
# Nmap 7.80 scan initiated Tue May  7 16:28:13 2024 as: nmap -O -sV -sT -sC -oN nmap26.log 10.15.42.36
Nmap scan report for 10.15.42.36
Host is up (0.036s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.18.0.3 is not the same as 10.15.42.36
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login Page
Aggressive OS guesses: Linux 2.6.32 (92%), Linux 3.1 (91%), Linux 3.2 (91%), AXIS 210A or 211 Network Camera (
Linux 2.6.17) (90%), Linux 2.6.39 - 3.2 (89%), Linux 3.1 - 3.2 (89%), Linux 3.2 - 4.9 (89%), Linux 3.7 - 3.10
(89%), Linux 3.8 (89%), Synology DiskStation Manager 5.1 (Linux 3.2) (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue May  7 16:28:35 2024 -- 1 IP address (1 host up) scanned in 21.83 seconds
```

Figure 1: Sample output of network scan

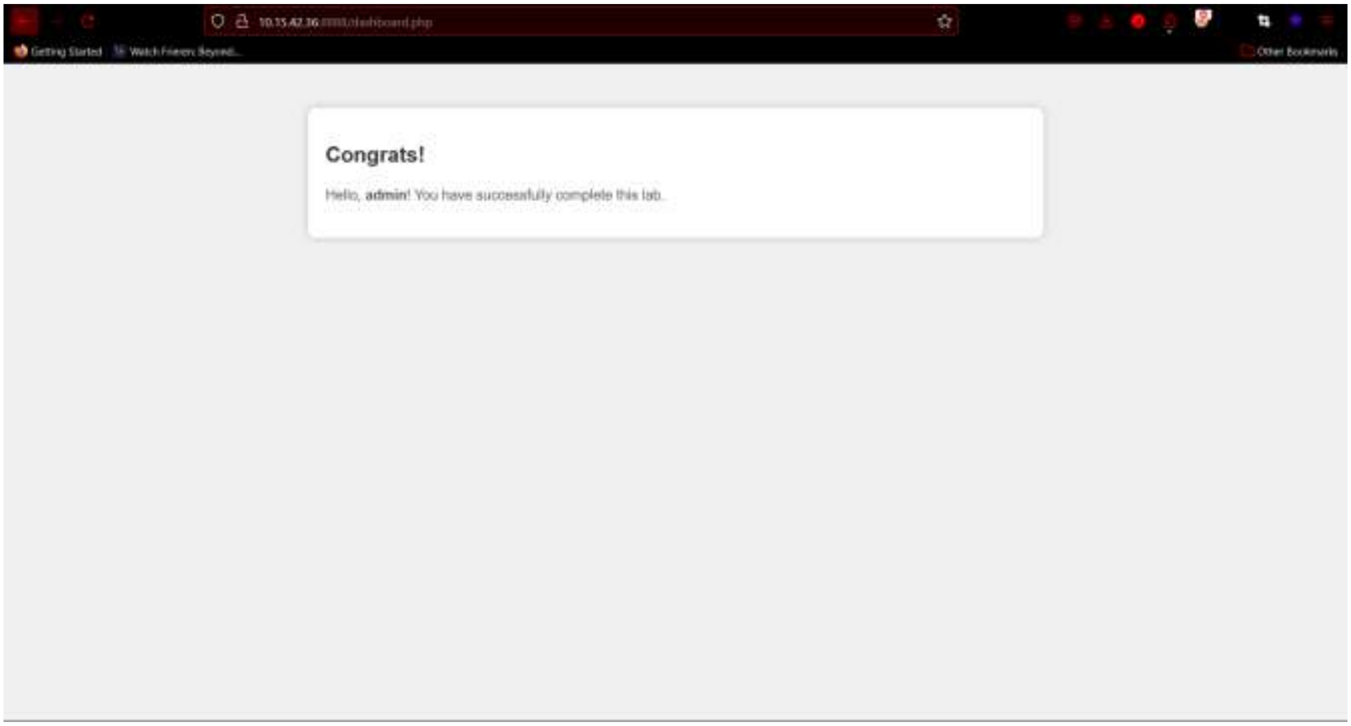
CyberShield used the gathered information to connect to the FTP service which requires no password. By listing the directory, CyberShield found a backup database that saved administrative credentials.



```
LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
```

Figure 2: Snippet of backup.sql database

CyberShield performed bruteforce on the hashed password using the rockyou.txt wordlist and found admin credentials (kiseki666).



Congrats!

Hello, **admin**! You have successfully complete this lab.

Figure 3: Successful admin login

CyberShield leveraged the valid credentials to log into admin.

Remediation

Who:	IT Team
Vector:	Remote
Action:	Configure FTP service by disabling anonymous access.

Additional Reports and Scans (Informational)

CyberShield provides all clients with all report information gathered during testing. This includes vulnerability scans. For more information, please see the following documents:

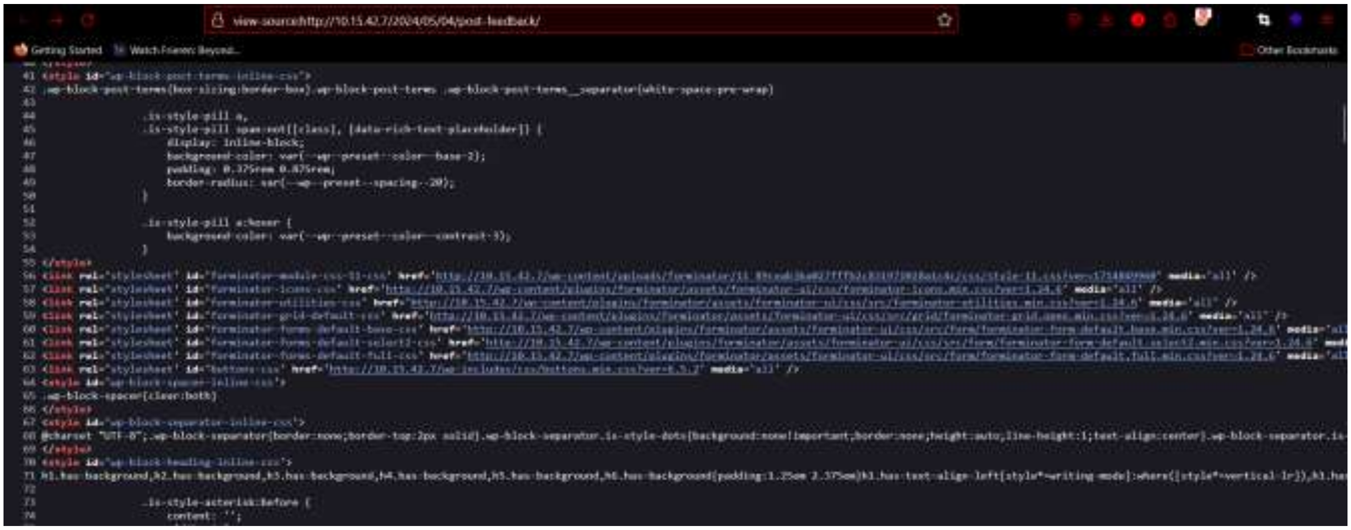
- Nmap36.log

WordPress Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution

Description:	Unauthenticated Remote Command Execution
Impact:	Critical (**CVSS Vector** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
System:	10.15.42.36
References:	https://www.exploit-db.com/exploits/51664 https://github.com/E1A/CVE-2023-4596

Exploitation Proof of Concept

CyberShield found information about wordpress plugin called forminator and its version by viewing source of http://10.15.42.7/2024/05/04/post-feedback/.



```
</style>
<style id="wp-block-post-terms-inline-css">
.wp-block-post-terms{box-sizing:border-box}.wp-block-post-terms .wp-block-post-terms__separator{white-space:pre-wrap}

                .is-style-pill a,
                .is-style-pill span:not([class], [data-rich-text-placeholder]) {
                    display: inline-block;
                    background-color: var(--wp--preset--color--base-2);
                    padding: 0.375rem 0.875rem;
                    border-radius: var(--wp--preset--spacing--20);
                }

                .is-style-pill a:hover {
                    background-color: var(--wp--preset--color--contrast-3);
                }
</style>
<link rel='stylesheet' id='forminator-module-css-11-css' href='http://10.15.42.7/wp-content/uploads/forminator/11_[illegible]/css/style-11.css?ver=[illegible]' media='all' />
<link rel='stylesheet' id='forminator-icons-css' href='http://10.15.42.7/wp-content/plugins/forminator/assets/forminator-ui/css/forminator-icons.min.css?ver=1.24.6' media='all' />
<link rel='stylesheet' id='forminator-utilities-css' href='http://10.15.42.7/wp-content/plugins/forminator/assets/forminator-ui/css/src/forminator-utilities.min.css?ver=1.24.6' media='all' />
<link rel='stylesheet' id='forminator-grid-default-css' href='http://10.15.42.7/wp-content/plugins/forminator/assets/forminator-ui/css/src/grid/forminator-grid.open.min.css?ver=1.24.6' media='all' />
<link rel='stylesheet' id='forminator-forms-default-base-css' href='http://10.15.42.7/wp-content/plugins/forminator/assets/forminator-ui/css/src/form/forminator-form-default.base.min.css?ver=1.24.6' media='al
<link rel='stylesheet' id='forminator-forms-default-select2-css' href='http://10.15.42.7/wp-content/plugins/forminator/assets/forminator-ui/css/src/form/forminator-form-default.select2.min.css?ver=1.24.6' medi
<link rel='stylesheet' id='forminator-forms-default-full-css' href='http://10.15.42.7/wp-content/plugins/forminator/assets/forminator-ui/css/src/form/forminator-form-default.full.min.css?ver=1.24.6' media='al
<link rel='stylesheet' id='buttons-css' href='http://10.15.42.7/wp-includes/css/buttons.min.css?ver=6.5.2' media='all' />
<style id="wp-block-spacer-inline-css">
.wp-block-spacer{clear:both}
</style>
<style id="wp-block-separator-inline-css">
@charset "UTF-8";.wp-block-separator{border:none;border-top:2px solid}.wp-block-separator.is-style-dots{background:none!important;border:none;height:auto;line-height:1;text-align:center}.wp-block-separator.is-
</style>
<style id="wp-block-heading-inline-css">
h1.has-background,h2.has-background,h3.has-background,h4.has-background,h5.has-background,h6.has-background{padding:1.25em 2.375em}h1.has-text-align-left[style*=writing-mode]:where([style*=vertical-lr]),h1.has

                .is-style-asterisk:before {
                    content: '';
```

Execute PoC script (https://github.com/E1A/CVE-2023-4596).

Last Page